Fisher Yüz Yöntemi Kullanılarak İki Aşamalı Doğrulama ile Yüz Algılama Tabanlı Güvenli ATM Sistemi

Dr.V.Praveena , Doçent,
praveenav@drngpit.ac.in Bilgisayar Bilimleri ve Mühendisliği Bölümü,
Dr.N.G.P. Teknoloji Enstitüsü,
Coimbatore

Aarthi S, Öğrenci,
aarthisivakumarr@gmail.com
Bilgisayar Bilimleri ve Mühendisliği Bölümü,
Dr.N.G.P. Teknoloji Enstitüsü,
Coimbatore

Anu Sankari S, Öğrenci,
19csanusankaris@drngpit.ac.in
Bilgisayar Bilimleri Bölümü ve Mühendislik,
Dr.N.G.P. Teknoloji Enstitüsü,
Coimbatore

Girija K, Öğrenci,
19csgirijak@drngpit.ac.in
Bilgisayar Bilimleri ve Mühendisliği Bölümü,
Dr.N.G.P. Teknoloji Enstitüsü,
Coimbatore

Kirthivarsini M, Öğrenci,
19cskirthivarsinim@drngpit.ac.in
Bilgisayar Bilimleri Bölümü ve Mühendislik,
Dr.N.G.P. Teknoloji Enstitüsü,
Coimbatore

2023 7th International Conference on Trends in Electronics and Informatics (ICOEI) | 979-8-3503-9728-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICOEI56765.2023.10125744

Özet **- Otomatik vezne makineleri (ATM'ler) günümüzde neredeyse herkes tarafından kullanılmaktadır. ATM kartını her yere taşımanın zorluğu nedeniyle, insanlar kartlarını veya PIN kodlarını yanlarında getirmeyi unutabilirler. ATM kartı kırılabilir ve bu da kullanıcının parasına erişimini kısıtlayabilir. Bu öneride gerçek bir güvenlik çözümü sunulmaktadır. Hesapların güvenliğini ve kullanıcıların gizliliğini artırmak için Yüz tanıma ve Mobil uygulama onayı gibi teknolojiler dahil edilmiştir. Bir kullanıcı yüzünü kaydettirdikten ve bankanın veritabanında sakladıktan sonra işlem yapmaya çalıştığında, sistem ATM'nin kamerasını kullanarak yüz algılama gerçekleştirir ve kullanıcı yüz doğrulaması yapar. Geçersiz kullanıcının işlem sürecine devam etmesi gerekiyorsa, OTP kimlik doğrulaması geçerli kullanıcı tarafından Mobil uygulamada yapılmalıdır, böylece yetkisiz kişi işleme devam edecektir.**

Anahtar Kelimeler - ATM (Otomatik Vezne Makinesi), Güvenlik, Yüz Tanıma, Mobil Uygulama, OTP (Tek Kullanımlık Şifre)

I.GİRİŞ

Bilim ve teknolojideki hızlı ilerlemenin genel anlamda iyi bir etkisi olmasına rağmen, çok sayıda finans kurumu hırsızlık ve dolandırıcılığın hedefi olmaya devam etmektedir. ATM'ler tüketicilerin finansal işlemlerini ve bankacılık ihtiyaçlarını karşılamak için her zaman hazırdır. ATM'nin temel avantajı, bankaya gitmek için zaman kaybetme ve işlem yapmak için sırada bekleme ihtiyacını ortadan kaldırmasıdır. ATM'ler, sağladığı kolaylıklar nedeniyle halk arasında büyük bir popülerlik kazanmıştır.

erişilebilirlik ve genel kullanıcı dostu olma. Mevcut ATM sistemi tarafından iki farklı hizmet sağlanmaktadır.

İlki tüketiciye sadece talep edilen parayı sağlamakla kalmaz, aynı zamanda alınan para miktarını ve hesap bakiyesini detaylandıran bir mesaj gönderir. İkincisi, kredi kartı ödemelerine izin vermesi, kullanıcı depozitolarını kabul etmesi ve kullanıcıyı işlemler ve hesap bilgileri hakkında bilgilendirmesi açısından daha ileri düzeydedir.

PIN tabanlı doğrulama, mevcut ATM güvenlik kimlik doğrulaması için bir gerekliliktir. Yalnızca hesaplarına erişmelerini sağlayan PIN'lerini (Kişisel Kimlik Numarası) bilen kişilerin ATM kullanmasına izin verilir. Otomatikleştirilmiş bir makine, bir güvenlik açığı nedeniyle savunmasız hale gelir. ATM üreticileri, müşterilerin bankacılık işlemlerini endişe veya zorluk yaşamadan gerçekleştirebilmeleri için sürekli olarak güvenlik özelliklerini geliştirmekte ve eklemektedir.

Kullanıcılara gerçek bir güvenlik çözümü sunmak amacıyla yüz tanımaya dayalı bir ATM güvenlik sistemi fikri ortaya çıkmıştır. Projenin

Ana hedef, hırsızlık ve sahte ATM kartlarının neden olduğu dolandırıcılığı azaltmaktır. Sistem size yapmak istediğiniz işlemi gerçekleştirme seçeneği sunacaktır. Kullanıcı tarafından "Yüz tanıma tabanlı işlem" seçeneğinin seçilmesi gerekmektedir. İşlem, veritabanı görüntüsüyle eşleşirse devam edecek; aksi takdirde durdurulacaktır. Kullanıcı, şube adını seçtikten ve görüntü eşleşirse doğrulamanın ikinci adımı için gerekli olan PIN kodunu girdikten sonra işleme devam edebilir. Bir mobil uygulama yardımıyla, geçerli bir kullanıcı, yetkisiz bir kullanıcının para çekmesini önlemek için bir OTP üretebilir. Geçersiz kullanıcı daha sonra işleme devam etmek için bu OTP'yi kullanabilir.

II. LİTERATÜR TARAMASI

Rashmi pote ve diğerleri[1], müşterilerin akıllı telefonlarını banka sunucusuna kaydettirdikten sonra banka portalı üzerinden Akıllı Mobil Bankacılık Uygulamasını (SMBA) yüklemeleri gerekmektedir. Müşteri, SMBA'dan nakit para çekmeye başlarken kimlik doğrulama olarak bir şifre kullanmaya karar vermelidir. Nakit çekme işlemleri, başlatıldıktan ve banka sunucusu şifreyi başarıyla doğruladıktan sonra bankanın veri tabanına işlenir. Müşteri, Kişisel Bilgileri Hızlı Yanıt (QR) Kodu ile aktarabilir ve ardından nakit parayı almak için en yakın ATM'yi ziyaret edebilir.

Gokul S, Kukan S, Meenakshi K, Vishnu Priyan S S, Rohan Gini J. M.E.Harikumar [2] RFID ve parmak izi yetkilendirmesi ATM'nin çalışmasının temelini oluşturmaktadır. Kullanıcının tanınan kart numarası, kimlik doğrulama durumu ve erişim konumu, veritabanı verilerine çapraz referans verilerek doğrulandıktan sonra, RFID numarası ve ayrıntıları onlardan alınır. Bilgiler doğrulandığında yetkilendirmenin gerçek olup olmadığı hesap sahibine bildirilir. Güvenlik nedeniyle, kişinin yüzü de tarih ve saat ile birlikte cihaz tarafından kameraya alınır.

J. Patoliya, Miral M, Desai [3], Gömülü Linux Platformu, Akıllı ATM Güvenlik Sistemi fikrinin temelini oluşturmaktadır. Genişletilmiş yeteneklere sahip görüntü işleme yazılımı OpenCV kullanılmıştır. kredi kartı büyüklüğünde bir Raspberry Pi kartı üzerinde oluşturuldu. Güvenliği sağlamak için önce bir insan yüzü yakalanır ve yüz tespitinin doğruluğu kontrol edilir. Eğer bu yapılamazsa, kullanıcı, yüzü doğru bir şekilde tanımlamak için konumunu değiştirmeye teşvik edilir. Buna rağmen, yüz pozitif olarak tanımlanamazsa, bekçinin cep telefonu numarasına SMS yoluyla 3 basamaklı bir OTP gönderilir. Bekçi tuş takımını kullanarak OTP'yi girdiğinde, ATM odasının kapısının kilidi açılacaktır; aksi takdirde kilitli kalacaktır.

Soundari D V, Aravindh R, Edwin Raj K, Abishek S [4], Bu fikir Face-id'yi mevcut tekniğe bir anahtar olarak dahil etmektedir. Her kişinin faceID'sinin benzersiz olması ve kullanıcıdan başkası tarafından kullanılamaması bir avantajdır. Yüz kimliği tarama uygulaması için makine öğrenimi ve görüntü işleme teknolojileri (Eigenface algoritması gibi) kullanılmaktadır.

Apurva Taralekar, Gopalsingh Chouhan, Rutuja Tangade, Nikhilkumar Shardoor [5], Parmak izleri benzersiz bir tanımlama biçimi olarak hizmet verdiği için mevcut en güvenli sistemlerden biri olan biyometrik parmak izi kimlik doğrulama yaklaşımı ile yetkisiz erişim yasaklanmıştır. Ayrıca, bu teknoloji güvenli bir GSM tabanlı işlemi (OTP) garanti eder. Geleneksel ATM sistemiyle karşılaştırıldığında, önerilen çözüm üstün güvenlik sağlamaktadır.

III. KARŞILAŞTIRMALI ÇALIŞMA

[1] "Akıllı Mobil Bankacılık Uygulaması yardımıyla ATM'den nakit para çekme güvenliğinin sağlanması" başlıklı makalede üç faktörlü kimlik doğrulama yaklaşımı önerilmektedir. Güvenlik amacıyla, kullanıcı bir şifre girerek SMBA'dan nakit para çekmeye başlayabilir. Tüketici yakındaki bir ATM'yi ziyaret edebilir ve QR kodunu tarayarak nakit parayı alabilir, bu da işlem süresini uzatır.

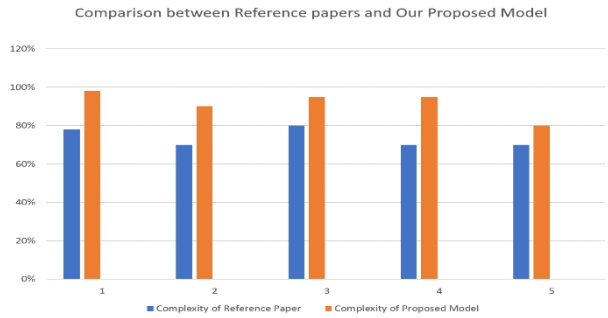
Müşteri nakit çekme işlemini başlattığında ve banka sunucusu müşterinin şifresini başarılı bir şekilde doğruladığında. Bizim önerdiğimiz yaklaşımda işlem, yüz tanındığında ve OTP girildiğinde gerçekleşir, bu da süreci hızlandırır.

[2] "Yüz Algılama Açık CV Tabanlı ATM Güvenlik Sistemi" başlıklı makale, PIN ve ATM kartı kullanımına alternatif olarak biyometrik tanımlama teknikleri önermektedir. Ancak, bizim fikrimizde ATM kartları kullanılmadığından, bunlardan birinin kopyalanması veya yanlış yerleştirilmesi durumunda daha az karmaşıktır.

[3] Artan parmak izi dolandırıcılığı sorunu ışığında, "IOT kullanan parmak izi sensörü ve RFID tabanlı ATM sistemi" makalesi, RFID ve parmak izi tanımlama kullanarak işlem yapmak için bir teknik önermektedir. Sistem önerimizde FaceID tabanlı tanıma uyguladık ve dolandırıcılığı pratik olarak imkansız hale getirdik.

[4] "RFID kullanan Biyometrik tabanlı Akıllı ATM" makalesine göre, işlem süreci yalnızca erişim izni verilen yerlerde gerçekleşebilir, çünkü devam etmeden önce ATM kart numarasının, yetkilendirme durumunun ve erişim konumunun doğrulanmasını gerektirir. Ancak, önerdiğimiz çözümdeki işlem prosedürü herhangi bir ATM makinesinde güvenilir bir şekilde gerçekleşebilir.

[5] Yüz tanıma aşamasından sonra OTP'nin oluşturulması zaman zaman gecikebilir (örneğin, belirli bir ağ hizmeti kapalıysa, kullanıcı OTP'yi alamayacaktır) ve bu da kullanıcıyı sabırsız hale getirir. "ATM Makinesi için OTP ile Geliştirilmiş Güvenlik" makalesi de işlem için ATM kartı gerektirir ve OTP, yüz tanındıktan sonra belirlenen cep telefonu numarasına bir kez gönderilir. Bu nedenle, sistemimizdeki zaman karmaşıklığını azaltmak için, kullanıcı bir aile üyesine veya arkadaşına para çekme yetkisi vermeden önce OTP'nin oluşturulduğu bir konsept önerdik.



Şekil 1 : Diğer makalelerin ve bizim önerdiğimiz modelin karmaşıklığının karşılaştırılması

IV. SİSTEM MİMARİSİ

A. MEVCUT SISTEM

Kullanıcıların çoğunluğu mevcut ATM'leri kullanmayı rahat ve kolay bulmaktadır. Mevcut ATM'ler tipik olarak ATM'nin etkileşimli çalışmasını sağlamak için kullanıcı tarafından okunan bir ATM ekranında talimatlar görüntüler. Kullanıcı, ekrandaki talimatları okuduktan sonra bir tuş takımına veri ve bilgi girerek ATM'yi kullanabilir ve çalıştırabilir. Pin tabanlı doğrulama yöntemi, mevcut ATM güvenlik kimlik doğrulama yönteminin bir gereğidir. Aciliyet ve istenmeyen pin paylaşımı da dahil olmak üzere birçok faktör sistem üzerinde etkilidir. Manyetik çipli kartların kopyalanması kolaydır.

Mevcut Sistemin Sınırlamaları

1. Omuz Sörfü

Omuz sörfü, bir kişiyi gözetlemek ve şifrelerini ve diğer kişisel bilgilerini öğrenmek amacıyla bir yazar kasa veya başka bir elektronik cihaz kullanarak izlemek için kullanılan bir tekniktir.

2. Spoofing

Başka birinin kimliğine bürünmek, hesabına erişim sağlamak ve bunu kötüye kullanmak sahteciliğe örnektir.

3. Kaymağı

Hırsızlar manyetik bir çipten kart bilgilerini elde etmek için kart kopyalama cihazları kullanırlar. Bu aygıtlar sıklıkla ATM kart okuyucusunun içine ya da üstüne yerleştirilir.

4. Kart Kimlik Avı

Müşteri alışveriş yapmak için kartını ATM'ye yerleştirdiğinde, kartı çalmak için bir kart kimlik avı girişiminde bulunulur. Müşterinin kartını ele geçirmek için kart yuvasının üstüne ya da içine bir aygıt yerleştirilir. Bu cihazlar, müşterilerin bir işlem sonrasında kartlarını geri almalarını engellemek için tasarlanmıştır.

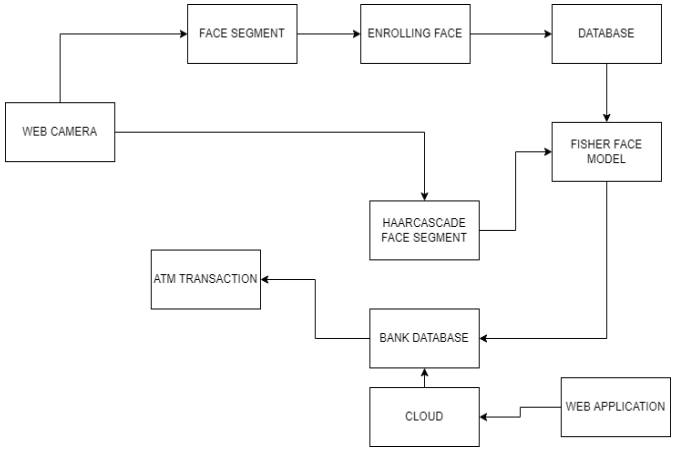
B. ÖNERILEN SISTEM

Yüz algılamaya dayalı bir ATM güvenlik sistemi fikri, halk için uygulanabilir bir güvenlik çözümü olarak geliştirilmiştir. Tanıma için yüzün dokusal özelliklerini çıkarmak için Haar- cascade ve Fisher Face kullanılır. Projemiz, bir bilgisayar görüşü çerçevesi kullanarak yüzleri tespit etmek için gömülü bir ATM kamerası kullanmayı amaçlamaktadır. Yüz algılama teknolojisi, kullanıcının yüzünü benzersiz bir şekilde tanımlamak için bir anahtar olarak kullanır. Otomatik Vezne Makineleri (ATM'ler) genellikle kullanıcı kimlik doğrulaması için pin tabanlı doğrulamaya dayanır. ATM'lerde tüketici kimlik doğrulamasının güvenliğini artırmak için çok sayıda çalışma yapılmıştır.

İlk durumda, müşterinin bankanın sunucusunda saklamak için yüzünü kaydetmesi ve bilgilerini kullanarak bankaya kaydolması gerekir. Veriler, verileri saldırılara karşı güvenli hale getiren bulutta şifrelenmiş biçimde saklanır.

Tüketici ikinci senaryoda yüz tanıma özelliğini kullanarak ATM'de bir işleme devam etmeyi seçtiğinde, arayüz Otomatik Vezne Makinesi'ne (ATM) yerleştirilmiş kamera yardımıyla kullanıcının yüzünü yakalar ve görüntünün eşleşip eşleşmediğini doğrulamak için veritabanıyla kontrol eder. Görüntü eşleşirse, kullanıcının şube adını seçmesi gerekir ve doğrulama için ikinci adım olarak verilen PIN kodunu girerek işleme devam edebilir.

Üçüncü senaryoda, geçerli kullanıcı yetkisiz kullanıcının parasını çekmesini isterse, mobil uygulama yardımıyla bir OTP oluşturabilir, bu nedenle geçersiz kullanıcı Şekil: 2'de verildiği gibi bu OTP yardımıyla işlemi gerçekleştirebilir.



Şekil 2 : Önerilen sistemin blok diyagramı

Bu modelin doğruluğu yüzden yüze değişmektedir ve genel doğruluk %93.5'tir ve yüzlerin tahmin süresi sisteme göre değişmektedir.

a) Fisher Faces Yüz Tanıma Algoritması

Eigenfaces yöntemi bu yöntem tarafından geliştirilmiştir. Eigenfaces, her kişiden gelen tüm eğitim yüzlerini bir kerede analiz eder ve ana yüzleri tanımlar. bileşenleri gelen her biri ayrı ayrı ele alınır. Bu şekilde, bir kişiyi diğerinden a y ı r a n özelliklere odaklanmaktan kaçınılmış olur.

Fisher Faces'ın yüz tanıma sistemi, bir kişiyi diğerlerinden ayıran temel özellikleri tam olarak çıkarır. Bu bağlamda, bir kişinin parçaları diğerlerini gölgede bırakmaz. Fisherface Temel Bileşenleri kullanır

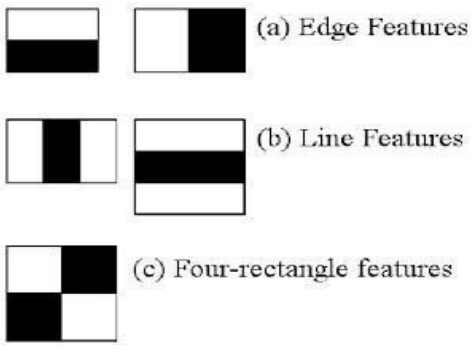
Analizi (PCA) ve Doğrusal Diskriminant Analizi (LDA) yöntemlerini kullanarak bir görüntünün özelliklerini çıkarır ve yüz uzayı boyutundaki azalmaya dayanarak yüzü tespit eder. Fisherface ayrıca bulanıklık ve gürültü kaynaklı resim etkilerine karşı da dayanıklıdır. FisherFace algoritması kullanılarak çeşitli insan ifadelerinin veya duygularının tanınma ve hesaplanma doğruluğu ölçülmüştür.

b) Haar Cascade Algoritması

Derin öğrenme, yüzleri tanımlamak için Haar Cascade yönteminde kullanılır. Yüz tespiti, bir kaskad fonksiyonunu eğitmek için çok sayıda hem pozitif hem de negatif fotoğraf kullanılarak mümkün hale getirilir.

Kamera bir fotoğraf çektikten sonra yapılması gereken ilk şey, görüntünün özelliklerini çıkarmaktır. Diyelim ki 8 × 8 piksellik tek bir görüntüden 160000'den fazla özellik çıkarmak istiyoruz. İkinci aşama, algoritmayı çok sayıda pozitif ve negatif fotoğrafla eğitmektir, çünkü yüz algılama tek bir görüntüden özellikler kullanılarak gerçekleştirilemez. Bir eşik değeri kullanılarak her görüntüden özellikler çıkarılır, ardından tüm özellikler birleştirilir ve algılama için kullanılır. 160000+ özellik bu noktada 6000 özelliğe indirgenir.

Sınıflandırıcılar özellik verilerinin küçük bir kısmını elde edilen görüntü ile değerlendirdiğinde, bir sonraki aşama yüz tespitidir. Seçilen özelliklerden herhangi biri elde edilen görüntü ile eşleşmezse Şekil:3'te görüldüğü gibi görüntü algılanmaz.



Şekil 3 : Haar Cascade Algoritmasının Özellikleri

V. SONUÇ

Durum 1 : Yüz eşleştiğinde

Müşteri, yüzün veritabanında kayıtlı resimle eşleşmesi durumunda şube adını seçebileceği işlemin bir sonraki adımına yönlendirilecektir.

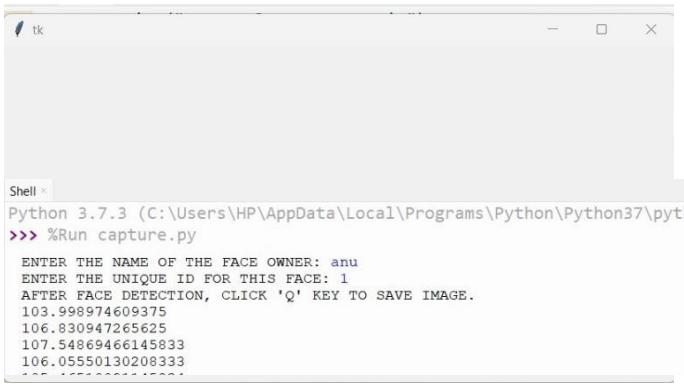
Durum 2 : Yüz eşleşmediğinde

Yüz eşleşmezse işleme devam edilmeyecektir.

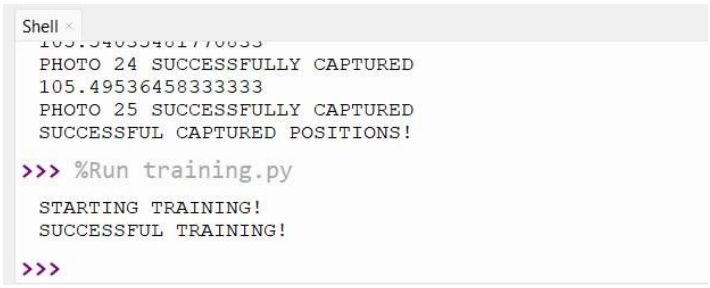
Durum 3 : Geçerli kullanıcı yetkisiz kullanıcının işlem yapmasını istediğinde

Yetkili kullanıcının bir işlem yapması gerekiyorsa, yetkili kullanıcı bir OTP üretmek için mobil uygulamayı kullanabilir ve yetkisiz kullanıcı daha sonra işlemi tamamlamak için bunu kullanabilir.

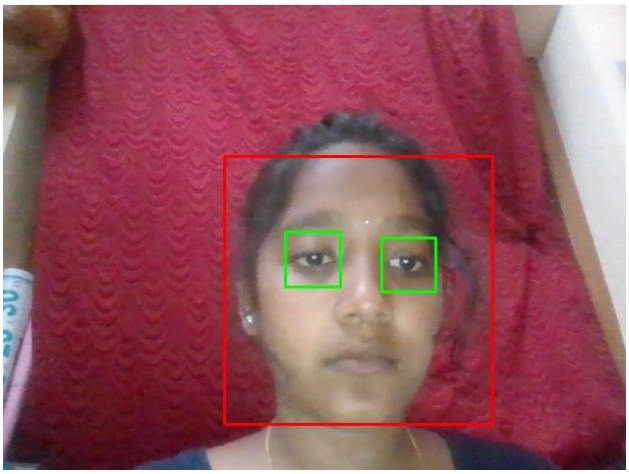
Şekil 4 : İşleme devam etmek için seçeneklerin görüntülenmesi



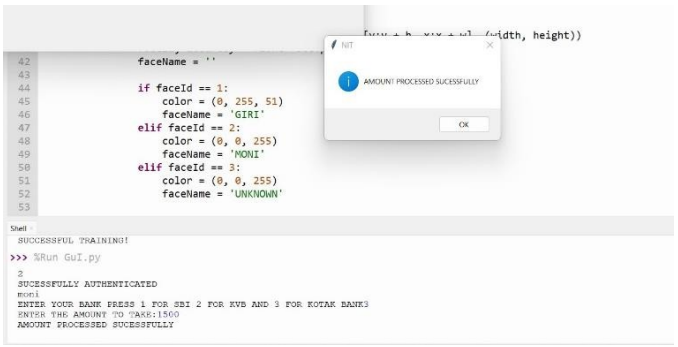
Şekil 5 : Yüzü yakalamadan önce detayların girilmesi.



Şekil 6 : Veri kümelerini başarıyla eğittikten sonra



Şekil 7 : Yüz yakalama



Şekil 8 : Banka seçildikten sonra tutar başarıyla işlenirse

Şekil 9 : Yetkisiz kullanıcılar için OTP ayarlama GUI'si işlem

VI. SONUÇ

ATM'ler için Biyometrik Kimlik Doğrulama, bireylere benzersiz bir şekilde bağlı olduğu için daha güçlü bir kimlik doğrulama ve onaylama yöntemidir. Daha fazla güvenlik sağlamak için OTP ile birlikte yüz tanıma yazılımı kullanan bir ATM tasarımı. Önerilen yöntem güvenli ve emniyetli işlemlere yardımcı olmaktadır. Bilgisayar korsanları, kamerayı ATM makinesinin yakınına sabitleyerek PIN numarasını kolayca kırabilir. ATM kartı da kopyalanabilir ve Yüz Tanıma Sistemi kullanılarak bunlar önlenebilir. PIN'i doğrulamanın ikinci adımı olarak kullanarak, sistem daha güvenli işlem gerçekleştirir. Yetkisiz kullanıcı, geçerli kullanıcı tarafından uygulamada oluşturulan OTP yardımıyla da işlem gerçekleştirebilir. İki seviyeli güvenlik sistemi ve geçerli kullanıcının uygulamada oluşturulan OTP yardımıyla geçersiz kullanıcının işlem yapmasına izin verebileceği bir özellik eklendiği için gerçekten kullanışlıdır.

VII. REFERANSLAR

[1] J.J. Patoliya, M.M. Desai, Gömülü Linux Platformu kullanan Yüz Algılama tabanlı ATM Güvenlik Sistemi, 2nd International Conference for Convergence in Technology (I2CT), 2017.

[2] M. Karovaliyaa, S. Karediab, S. Ozac, Dr.D.R. Kalbande, ATM makinesi için OTP ve Yüz Tanıma Özellikleri ile Geliştirilmiş Güvenlik, International Conference on Advanced Computing Technologies and Applications (ICACTA), 2015.

[3] Sivakumar T, Gajjala Askok, Sai Venu, Design and Implementation of Security Based ATM theft Monitoring System, International Journal of Engineering Inventions, Volume 3, Issue 1, 2013.

[4] C.Bhosale, P.Dere, C.Jadhav, ATM security usingface and fingerprint recognition, International Journal of Research in Engineering, Technologyand Science, Volume VII, Special Issue, Feb 2017.

[5] Manoj V, M.Sankar R, Sasipriya S, U.Devi E, Devika T, Multi Authentication ATM Theft Prevention Using iBeacon , International Research Journal of Engineering and Technology (IRJET).

[6] L.Wang, H.Ji, Y.Shi, Maksimum Yerel Fisher Diskriminant Analizi Kullanarak Yüz Tanıma, 18. IEEE Uluslararası Görüntü İşleme Konferansı, 2011.

[7] K.Shailaja, Dr. B.Anuradha, Etkili DeepLearning kullanarak Yüz Tanıma temelli Doğrusal Diskriminant Sınıflandırma, IEEE International Conference on ComputationalIntelligence and Computing Research, 2016.

[8] H.R.Babaei, O.Molalapata ve A.H.Y.Akbar Pandor, Otomatik Vezne Makineleri (ATM) için Yüz Tanıma Uygulaması, International Conference on Information and Knowledge Management (ICIKM), 2012.

[9] Rutuja Naval, Ankita Khot, Samruddhi Khedekar , Manjushree Sangale, Securing ATM Transaction OTP and Facial Recognition Features, International Journal of Advanced Research in Science, Communication Technology (IJARSCT), Volume 2, Issue 8, June 2022.

[10] DR S Sasipriya, Dr P Mayil Vel Kumar, S.Shenbagadevi, Yüz Tanıma Tabanlı Yeni Nesil ATM Sistemi, European Journal of Molecular and Clinical Medicine, Cilt 7, Sayı 4, 2020.

[11] Bharti Thakur,Pof. Bhupinder Verma, "Smart-Vision ile ATM Güvenliği Tasarımı",2018 Uluslararası Akıllı Devreler ve Sistemler Konferansı (ICICS)

[12] S Gokul,S Kukan,K Meenakshi,S S Vishnu Priyan,J Rolant Gini,M.E. Harikumar, RFID Kullanan Biyometrik Tabanlı Akıllı ATM, Üçüncü Uluslararası Akıllı Sistemler ve Buluşçu Teknoloji Konferansı (ICSSIT), 2020.

[13] S. Shriram, Swastik B. Shetty, Vishnuprasad P. Hegde,K C R Nisha,V. Dharmambal, Smart ATM surveillance system, International Conference on Circuit Power and Computing Technologies (ICCPCT), 2016.

[14] Soundari D V,Aravindh R,Edwin Raj K,Abishek S, Yüz Tanıma Yoluyla ATM'lerin Gelişmiş Güvenlik Özelliği, 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021.

[15] Maddela Subha Sri,J.Krishna Chaithanya,Nelli Dhruthiee, IDLE Uygulaması Altında Akıllı ATM Tasarımı ve Uygulaması, 7. Uluslararası İletişim ve Elektronik Sistemler Konferansı (ICCES), 2022